Załącznik Nr 1 OPZ- specyfikacja techniczna do SWZ
po modyfikacji

OPIS PRZEDMIOTU ZAMÓWIENIA – SPECYFIKACJA TECHNICZNA

Zadanie 1. Dostawa biblioteki taśmowej.
Zadanie 2. Dostawa hybrydowych komputerów przenośnych.
Zadanie 3. Dostawa sprzętu komputerowego.
Zadanie 4. Dostawa serwera plików wraz z dyskami.
Zadanie 5. Dostawa licencji oprogramowania systemu antywirusowego.

Spis treści

1. Dostawa biblioteki taśmowej.

1.1 Ilości.

SPRZĘT	ILOŚĆ
Biblioteka taśmowa LTO w obudowie RACK	1 szt.

1.2 Postanowienia ogólne.

Przedmiotem niniejszego zamówienia jest dostawa biblioteki taśmowej LTO w obudowie RACK na potrzeby Starostwa Powiatowego w Kielcach wraz z dodatkowym wyposażeniem. Dostawa wraz z usługą fizycznej instalacji oraz konfiguracją urządzenia. W ramach usługi zostanie wykonana m.in.:
- aktualizacja firmware,
- podłączenie do aktualnie istniejącej infrastruktury (oprogramowanie VEEAM, interfejs biblioteki taśmowej Fibre Channel, FC 8 Gb),
- konfgruacja kolejek backupowych,
- testowe odtworzenie,

Dostawa obejmuje wyspecyfikowane poniżej elementy.

1.2.1 Opis parametrów technicznych sprzętu objętego dostawą na potrzeby Starostwa Powiatowego w Kielcach.

1.2.2 Biblioteka taśmowa LTO w obudowie RACK

	Nazwa komponentu	Wymagane parametry techniczne urządzenia
1.	Typ Biblioteki	Biblioteka taśmowa w obudowie RACK 3U
2.	Typ zainstalowanego napędu	LTO-8 FC
3.	Liczba zainstalowanych napędów	2
4.	Liczba obsługiwanych napędów	Min. 1, maks: 21
5.	Liczba obsługiwanych slotów	Min. 20, maks 280
6.	Liczba dostarczonych aktywnych slotów	40

	Nazwa komponentu	Wymagane parametry techniczne urządzenia
7.	Zapis i odczyt danych	• Zapis danych: Min. 300 MB/s; • Odczyt danych: Min. 750 MB/s.
8.	Funkcje i obsługa	• Wbudowany skaner kodów paskowych na nośnikach LTO; • Lokalne zarządzanie za pomocą panelu/pulpitu operatora; • Obsługa szyfrowania danych na nośniku LTO; • Obsługa nośników LTO RW oraz LTO WORM; • Gwarantowana kompatybilność odczytu taśm LTO-7; • Gwarantowana kompatybilność zapisu taśm LTO-7.
9.	Interfejs zdalnego zarządzania	Ethernet 10/100/1000 Mb/s złącze RJ-45.
10.	Gwarancja i wsparcie	• 60 miesięczny okres gwarancji; • Realizowana w miejscu instalacji sprzętu, gwarantowana wizyta certyfikowanego serwisanta producenta w miejscu użytkowania sprzętu do końca następnego dnia roboczego od zgłoszenia; • Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta – dokumenty potwierdzające załączyć do oferty.
11.	Wyposażenie	• 1 nośnik czyszczący LTO; • 25 nośników LTO-8 RW dedykowanych do oferowanej macierzy z dołączona etykietą zawierającą kod kreskowy, • każdy nośnik z dołączoną etykietą zawierającą kod kreskowy
12.	Certyfikaty	EN 62368-1, IEC 62368-1, IEC 60950-1, EN 61000-3-3, EN 61000-3-2, ICES 003 Class A, FCC Part-15 Class A, VCCI Class A, RoHS, Weee, CE.

2. Dostawa hybrydowych komputerów przenośnych.

2.1 Ilości.

SPRZĘT	ILOŚĆ
Hybrydowy komputer przenośny	2 szt.

2.2 Postanowienia ogólne.

Przedmiotem niniejszego zamówienia jest dostawa hybrydowych komputerów przenośnych oraz oprogramowania typu OEM przypisanego do tego sprzętu komputerowego. Dostawa hybrydowych komputerów przenośnych oraz licencji obejmuje wyspecyfikowane poniżej elementy.
Postępowanie prowadzone jest w formie zadania, którym jest dostawa wszystkich wymaganych przez Zamawiającego komponentów sprzętu komputerowego.

W momencie odbioru zamawiający przewiduje możliwość zastosowania procedury sprawdzającej legalność dostarczonego oprogramowania. Ponadto zamawiający dopuszcza możliwość przeprowadzenia weryfikacji oryginalności dostarczonych programów komputerowych u Producenta oprogramowania w przypadku wystąpienia wątpliwości co do jego legalności.

2.3 Opis parametrów technicznych sprzętu objętego dostawą na potrzeby Starostwa Powiatowego w Kielcach.

2.3.3 Hybrydowy komputer przenośny – 2 szt.

Lp.	Nazwa komponentu	Wymagane parametry techniczne urządzenia
1.	Typ	• Hybrydowy Komputer przenośny typu laptop/ultrabook z dotykowym ekranem oraz z dołączaną klawiaturą; • W ofercie należy podać nazwę producenta, typ, model oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.
2.	Zastosowanie	• Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
3.	Ekran	• Matryca dotykowa min. 13" – max 14" błyszcząca z podświetleniem LED, zalecana rozdzielczość min. 2880 x 1920; • Częstotliwość odświeżania: min 120 Hz; • Jasność matrycy: min. 450 cd/m^2.
4.	Płyta główna	• Wyposażona przez producenta w dedykowany chipset dla oferowanego procesora. Zaprojektowana na zlecenie producenta, oznaczona trwale na etapie produkcji nazwą lub logiem producenta oferowanego komputera;

		• Wbudowana karta sieciowa WiFi min. 6E; • Wbudowany moduł bluetooth min. 5.1; • Wbudowany min. 1x: ✓ Akcelerometr ✓ Magnetometr ✓ Żyroskop
5.	Procesor	• Procesor dla urządzeń mobilnych; • Wydajność obliczeniowa: procesor powinien osiągać w teście benchmark, według wyników opublikowanych na stronie www co najmniej wynik 13.500 punktów. Wynik dostępny na stronie: http://www.cpubenchmark.net.
6.	Pamięć RAM	• Min. 16 GB typu LPDDR5, min. 4800 MHz, wlutowana.
7.	Dysk twardy	• Min. 512 GB klasy SSD, M.2 PCIe.
8.	Karta graficzna	• Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej w trybie UMA (Unified Memory Access); • Oferowana karta graficzna musi osiągać w teście PassMark G3D Mark co najmniej wynik 2.400. Wynik dostępny na stronie: http://www.videocardbenchmark.net.
9.	Multimedia	• Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition Audio; • Wbudowane głośniki; • Wbudowana kamera na podczerwień min. 2.1 Mpix; • Dodatkowa kamera min. 10.0 Mpix; • Wbudowane min. 2x mikrofony.
10.	Obudowa	• Aluminiowa z rozkładaną podstawką; • Wymiary maks: 1 cm x 30 cm x 24 cm (wys. x szer. x dł.); • Dopuszczalne kolory: czarny, szary, srebrny, grafit.
11.	Porty/złącza	• USB Typu-C (z Thunderbolt™ 4) - 2 szt.; • Złącze stacji dokującej - 1 szt.; • Surface Connect - 1 szt.; • Wymagana ilość portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
12.	Napęd optyczny	• brak
13.	Zasilanie	• Bateria zapewniająca pracę po naładowaniu na min. 10 godzin pracy; • Zasilacz zewnętrzny dedykowany.
14.	Klawiatura	• Dołączana i odłączana z interfejsem magnetycznym; • Kompatybilność min. : Microsoft Surface Pro 8, Microsoft Surface Pro X, lub równoważny Układ polski programisty, US –QWERTY; • Klawisze funkcyjne; • Miejsce na pióro/rysik, dołączony rysik w komplecie • Waga maks: 320 g; • Wymiary maks: Szerokość: 30 cm, Głębokość: 24 cm, Wysokość: 0,6 cm.
15.	System operacyjny	• Zainstalowany system operacyjny **Windows 10 Home / Windows 10 Pro** lub **Windows 11 Home/ Windows 11 Pro** .

		Klucz licencyjny Windows musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego na podstawie dołączonego nośnika bezpośrednio z wbudowanego napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego. Oferowany dostarczony system jak i również jego reinstalacja nie może wymagać aktywacji klucza licencyjnego za pośrednictwem telefonu i Internetu; • Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim;
16.	Oprogramowanie dodatkowe	• Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci; • Partycja recovery (opcja przywrócenia systemu z dysku).
17.	Bezpieczeństwo	• Moduł TPM lub równoważny.
18.	BIOS	• BIOS zgodny ze specyfikacją UEFI.
19.	Certyfikaty i standardy	• Deklaracja zgodności CE (załączyć do oferty); • Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS (załączyć do ofert); • Potwierdzenie poprawnej współpracy komputera z systemem operacyjnym - Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację.
20.	Waga	• Waga urządzenia z baterią podstawową nie większa niż 1,0 kg.
21.	Gwarancja	• Co najmniej 12-miesięczna gwarancja producenta, świadczona w siedzibie Zamawiającego na miejscu, w przypadku gdy konieczna będzie naprawa sprzętu w siedzibie producenta lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu pokrywa Wykonawca, • W przypadku wymiany dysku twardego uszkodzony dysk pozostaje u Zamawiającego, klienta; • Karta gwarancyjna producenta i warunki gwarancji dostarczone wraz ze sprzętem, obejmujące wszystkie opcje serwisowe wymagane przez Zamawiającego; • Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
22.	Wymagania dodatkowe	• Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu.

3. Dostawa sprzętu komputerowego.

3.1 Ilości.

SPRZĘT	ILOŚĆ
Komputer typu All-In-One	30 szt.

Komputer przenośny - laptop	10 szt.
Telefon stacjonarny VOIP	12 szt.
Drukarka przenośna, atramentowa	1 szt.
Pamięć RAM 16 GB dedykowana	10 szt.

3.2 Postanowienia ogólne.

Przedmiotem niniejszego zamówienia jest dostawa sprzętu komputerowego oraz oprogramowania typu OEM przypisanego do tego sprzętu komputerowego. Dostawa sprzętu komputerowego oraz licencji obejmuje wyspecyfikowane poniżej elementy.
Postępowanie prowadzone jest w formie zadania, którym jest dostawa wszystkich wymaganych przez Zamawiającego komponentów sprzętu komputerowego.

W momencie odbioru zamawiający przewiduje możliwość zastosowania procedury sprawdzającej legalność dostarczonego oprogramowania. Ponadto zamawiający dopuszcza możliwość przeprowadzenia weryfikacji oryginalności dostarczonych programów komputerowych u Producenta oprogramowania w przypadku wystąpienia wątpliwości co do jego legalności.

3.3 Opis parametrów technicznych sprzętu objętego dostawą na potrzeby Starostwa Powiatowego w Kielcach.

3.3.1 Komputer typu AiO (All-in-One) – 38 szt.

Lp.	Nazwa komponentu	Wymagane parametry techniczne urządzenia
1.	Typ	• Komputer stacjonarny typu All-in-One; • W ofercie wymagane jest podanie modelu, symbolu oraz producenta.
2.	Zastosowanie	• Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja programistyczna.
3.	Procesor	• Procesor zaprojektowany do pracy w komputerach typu all-in-one lub laptopach (w obudowie BGA o obniżonym współczynniku TDP) z dedykowanym chłodzeniem aktywnym; • Procesor wielordzeniowy - minimum 6 rdzeni fizycznych; • Wydajność obliczeniowa: procesor powinien osiągać w teście wydajności PassMark – CPU Mark wynik min. 18.000 punktów z dnia ..... według wyników ze strony https://www.cpubenchmark.net.
4.	Pamięć RAM	• Pamięć operacyjna: min. 8 GB, DDR4, bez korekcji błędów

		ECC; • Możliwość rozbudowy do min. 32 GB.
5.	Płyta główna	• Płyta główna zaprojektowana i wyprodukowana na zlecenie producenta komputera, trwale oznaczona logo producenta oferowanej jednostki, dedykowana dla danego urządzenia; wyposażona w - min. 2 złącza DIMM z obsługą do 32GB DDR4 pamięci RAM, - min. 1 złącza M.2 2280 dla dysku twardego, - min. 1 złącze M.2 karty WiFi; • Cechy dodatkowe: - Zintegrowana karta dźwiękowa, zgodna z High Definition Audio, - Wbudowany w płytę lub zewnętrzny moduł TPM połączony za pomocą dedykowanego portu, zamontowany na stałe w obudowie, - Wbudowana karta LAN 10/100/1000 Mbit/s, - Karta sieciowa WiFi 6E z Bluetooth 5.2; • Min. 2 sloty pamięci RAM, w tym min. 1 wolny; • Wymagana ilość portów lub złączy nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
6.	Dysk twardy	• Min. 256 GB, typu SSD, NVMe.
7.	Grafika	• Karta graficzna zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej w trybie UMA (Unified Memory Access); • Oferowana karta graficzna musi osiągać w teście PassMark G3D Mark co najmniej wynik 1.800 punktów, wynik dostępny na stronie: http://www.videocardbenchmark.net.
8.	Wyposażenie	• Wbudowane min. dwa głośniki o mocy min. 2W każdy; • Wbudowana kamerka min. 1.0 MPx; • Wbudowany mikrofon; • Dołączona w komplecie klawiatura USB w układzie polski programisty, z wydzielonym blokiem numerycznym, układ US –QWERTY, przewodowa; • Dołączona w komplecie mysz optyczna USB, przewodowa; • Przewody zasilające;
9.	Obudowa	• Typu All-in-One zintegrowana z matrycą min. 23,8"; • Obudowa plastikowa lub metalowa; • Kolory dopuszczalne: Czarny, szary, srebrny, grafit, biały; • W obudowie wbudowane min. 1 dioda sygnalizująca stan zasilania; • Demontaż tylnej pokrywy musi odbywać się bez użycia narzędzi, nie dopuszcza się stosowania śrub motylkowych, radełkowych czy zwykłych wkrętów; • Możliwość zastosowania zabezpieczenia fizycznego w postaci linki metalowej; • Każdy komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszonym na obudowie, oraz musi

		być wpisany na stałe w BIOS; • Zamawiający nie dopuszcza połączenia matrycy z płytą główną komputera poza jego obudową za pomocą dodatkowych przewodów; • Zamawiający nie dopuszcza połączenia wewnętrznych głośników z płytą główną za pomocą złącza USB, minijack/jack; • Wymagana ilość portów lub złączy nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.; • Wbudowane porty: Panel tylny : - 1x HDMI - 1x RJ45 Ethernet port - 2x USB 3.2 Gen 1 typ A z Smart Power On - 1x USB 3.2 Gen 2 typ A - 1x Uniwersalny audio port (combo) lub 1x port słuchawki - 1x gniazdo zasilania (Nie dopuszcza się portów USB usytuowanych na dolnej krawędzi obudowy z racji na ergonomię pracy a w szczególności regulację wysokości); • Nie dopuszcza się stosowania rozgałęziaczy, hubów itp.; • Możliwość instalacji dodatkowego dysku twardego 2,5" wewnątrz komputera.
10.	Matryca	• IPS, Full HD, min. 23,8", zalecana rozdzielczość min. 1920 x 1080, powłoka przeciwodblaskowa, wbudowana w obudowę komputera, nie dotykowa; • Kąty widzenia poziom/pion min. 178/178; • Kontrast min.: 1000:1; • Jasność min. : 250 cd/m²; • Czas reakcji: maks. 14 ms.
11.	Zasilanie	• Zasilacz wewnętrzny o mocy zalecanej przez producenta, dedykowany, o efektywności min. 85% przy obciążeniu zasilacza na poziomie 50%; • Zasilacz w oferowanym komputerze musi spełniać wymogi 80plus.
12.	Ergonomia	• Suma wymiarów obudowy z zainstalowanym standem nie może przekraczać: 112 cm;
13.	Bezpieczeństwo	• Komputer wyposażony w moduł TPM 2.0; • Złącze typu Kensington Lock lub równoważne; • Płyta główna zawierająca układ sprzętowy służący do tworzenia i zarządzania wygenerowanymi przez komputer kluczami szyfrowania. Zabezpieczenie to musi posiadać możliwość szyfrowania poufnych dokumentów przechowywanych na dysku twardym przy użyciu klucza

		sprzętowego; • Czujnik otwarcia obudowy, musi zbierać zdarzenia i zapisywać je w BIOS.
14.	BIOS	• BIOS zgodny ze specyfikacją UEFI, wyprodukowany przez producenta komputera, zawierający logo lub nazwę producenta komputera lub nazwę modelu oferowanego komputera. Pełna obsługa BIOS za pomocą myszy. (przez pełną obsługę za pomocą myszy rozumie się możliwość swobodnego poruszania się po menu we/wy oraz wł/wy funkcji bez używania klawiatury); • Informacje dostępne z poziomu BIOS na potrzeby inwentaryzacji: wersja BIOS, nr seryjny, data produkcji komputera, pamięć RAM (taktowanie, wielkość, obsadzenie kości w slotach, procesor (nazwa, typowa prędkość, minimalna, maksymalna, cache L2 i L3), pojemności zainstalowanego lub zainstalowanych dysków twardych, MAC adres zintegrowanej karty sieciowej, zintegrowany układ graficzny, kontroler audio. Informacje dostępne w samym menu BIOS bez stosowania dodatkowego oprogramowania jak i wbudowanego systemu diagnostycznego; • Możliwość, ustawienia hasła na poziomie: – administratora [hasło nadrzędne] umożliwiające logowanie do BIOS, dokonywanie zmian, rozruch komputera, – użytkownika/systemowego [hasło umożliwiające użytkownikowi zmianę swojego hasła, zgodnie z uprawnieniami nadanymi przez administratora dokonywać lub nie zmian ustawień BIOS], rozruch systemu operacyjnego [hasło blokuje start systemu operacyjnego], – hasło dla dysku; • Funkcja blokowania/odblokowania BOOT-owania stacji roboczej z zewnętrznych urządzeń; • Możliwość wyłączenia/włączenia karty sieciowej, kontrolera SATA, kontrolera audio, głośników, kamery, mikrofonów, układu TPM, czytnika kart multimedialnych; • Możliwość włączenia/wyłączenia czujnika otwarcia obudowy, ustawienia go w tryb cichy; • Możliwość przypisania w BIOS numeru nadawanego przez Administratora oraz możliwość weryfikacji tego numeru w oprogramowaniu diagnostyczno-zarządzającym. Musi umożliwiać znaki specjalne: # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | };

		• Możliwość ustawienia portów USB w trybie „no BOOT", czyli podczas startu komputer nie wykrywa urządzeń bootujących typu USB, natomiast po uruchomieniu systemu operacyjnego porty USB są aktywne; • Możliwość wyłączania portów USB grupami oraz w szczególności pojedynczo w dowolnej kombinacji; • BIOS musi nanosić automatycznie wszystkie zmiany konfiguracji dotyczące w szczególności: pamięci, procesora, dysku.
15.	System operacyjny	• Zainstalowany system operacyjny **Windows 10 Pro** lub **Windows 11 Pro** . Klucz licencyjny Windows musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego na podstawie dołączonego nośnika bezpośrednio z wbudowanego napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego. Oferowany dostarczony system jak i również jego reinstalacja nie może wymagać aktywacji klucza licencyjnego za pośrednictwem telefonu i Internetu; • Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim;
16.	Dodatkowe oprogramowanie	• Zaimplementowany w BIOS system diagnostyczny z graficznym interfejsem użytkownika dostępny z poziomu BIOS lub szybkiego menu bootowania, umożliwiający przetestowanie w celu wykrycia usterki zainstalowanych komponentów bez konieczności uruchamiania systemu operacyjnego. System musi posiadać wszystkie swoje funkcjonalności w przypadku: braku dysku, uszkodzenia dysku, sformatowania dysku, braku dostępu do sieci, internetu. Nie dopuszcza się stosowania wewnętrznych i zewnętrznych urządzeń w celu uzyskania funkcjonalności systemu diagnostycznego jak również pobierania oprogramowania i instalacji na dysku czy w BIOS; • Oprogramowanie z nieograniczoną czasowo licencją na użytkowanie umożliwiające: - upgrade i instalacje wszystkich sterowników, aplikacji dostarczonych w obrazie systemu operacyjnego producenta, BIOS-u z certyfikatem zgodności producenta do najnowszej dostępnej wersji; - sprawdzenie przed zainstalowaniem wszystkich sterowników, aplikacji oraz BIOS bezpośrednio na stronie producenta przy użyciu połączenia internetowego z automatycznym przekierowaniem w celu uzyskania informacji o: poprawkach i usprawnieniach dotyczących aktualizacji, dacie wydania ostatniej aktualizacji, priorytecie aktualizacji, zgodności z systemami operacyjnymi, - włączenie/wyłączenie funkcji automatycznego restartu

		w przypadku, kiedy jest wymagany przy instalacji sterownika, aplikacji;
17.	Wymagania dodatkowe	• Sprzętowe wsparcie technologii wirtualizacji realizowane łącznie w procesorze, chipsecie płyty głównej oraz w BIOS systemu (możliwość włączenia/wyłączenia sprzętowego wsparcia wirtualizacji); • Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu.
18.	Certyfikaty i standardy	• Deklaracja zgodności CE (załączyć do oferty); • Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS (załączyć do ofert); • Potwierdzenie poprawnej współpracy komputera z systemem operacyjnym - Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację.
19.	Gwarancja	• Na okres co najmniej 36 miesięcy - świadczona w siedzibie Zamawiającego, chyba że niezbędna będzie naprawa sprzętu w siedzibie producenta lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca; • W przypadku wymiany dysku twardego uszkodzony dysk pozostaje u Zamawiającego; • Karta gwarancyjna producenta i warunki gwarancji dostarczone wraz ze sprzętem, obejmujące wszystkie opcje serwisowe wymagane przez Zamawiającego; • Zamawiający wymaga dedykowanego portalu producenta, który ma zapewnić dostęp do bazy wiedzy i narzędzi wsparcia technicznego; • Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta; • możliwość weryfikacji na stronie producenta posiadanej/wykupionej gwarancji.

3.3.2 Komputer przenośny – laptop – 10 szt.

Lp.	Nazwa komponentu	Wymagane parametry techniczne urządzenia
1.	Typ	• Komputer przenośny typu laptop/ultrabook; • W ofercie należy podać nazwę producenta, typ, model oraz numer katalogowy oferowanego sprzętu umożliwiający jednoznaczną identyfikację oferowanej konfiguracji.
2.	Zastosowanie	• Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, aplikacji obliczeniowych, dostępu do Internetu oraz poczty elektronicznej.
3.	Ekran	• Matryca min. 15.6" – max 16" z podświetleniem LED FHD i powłoką przeciwodblaskową, wymagana rozdzielczość min. 1920 x 1080.
4.	Płyta główna	• Wyposażona przez producenta w dedykowany chipset dla

		oferowanego procesora. Zaprojektowana na zlecenie producenta, oznaczona trwale na etapie produkcji nazwą lub logiem producenta oferowanego komputera, wyposażona w złącze M.2 PCIe oraz obsługująca standard USB 2.0/3.0/3.2; • Wbudowana karta sieciowa WiFi, pracująca w standardzie co najmniej 802.11 a/b/g/n/ac; • Wbudowany moduł bluetooth.
5.	Procesor	• Procesor dla urządzeń mobilnych; • Wydajność obliczeniowa: procesor powinien osiągać w teście benchmark, według wyników opublikowanych na stronie www co najmniej wynik 6000 punktów. Wynik dostępny na stronie: http://www.cpubenchmark.net.
6.	Pamięć RAM	• Min. 16 GB DDR4.
7.	Dysk twardy	• Min. 240 GB klasy SSD, standard min. SATA III, złącze M.2 PCIe.
8.	Karta graficzna	• Zintegrowana w procesorze z możliwością dynamicznego przydzielenia pamięci systemowej w trybie UMA (Unified Memory Access); • Oferowana karta graficzna musi osiągać w teście PassMark G3D Mark co najmniej wynik 1.000 punktów, wynik dostępny na stronie: http://www.videocardbenchmark.net.
9.	Multimedia	• Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition Audio; • Wbudowana kamera min. 0.92 Mpix oraz mikrofon.
10.	Obudowa	• Wymiary maks: 3 cm x 40 cm x 30 cm (wys. x szer. x dł.); • Dopuszczalne kolory: czarny, szary, srebrny, grafit, biały.
11.	Porty/złącza	• Wbudowane porty i złącza min.: • USB 2.0 – 1 szt. • USB 3.0 – 2 szt. • Wyjście HDMI – 1 szt. • Audio jack: typ combo – 1 szt. • RJ-45 (LAN) 1 Gb/s - 1 szt. • Wejście zasilania; • Wymagana ilość portów nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.
12.	Napęd optyczny	• Opcjonalny.
13.	Zasilanie	• Bateria – litowo-jonowa o pojemności co najmniej 3200 mAh, • Zasilacz zewnętrzny dedykowany.
14.	Klawiatura	• Wbudowana klawiatura standardowa lub z wydzielonym blokiem numerycznym, układ US–QWERTY.
15.	Urządzenia wskazujące	• TouchPad z obsługą sterowania dotykowego.
16.	System operacyjny	• Zainstalowany system operacyjny **Windows 10 Pro** lub **Windows 11 Pro** . Klucz licencyjny Windows musi być zapisany trwale w BIOS i umożliwiać instalację systemu operacyjnego na podstawie dołączonego nośnika bezpośrednio z wbudowanego napędu lub zdalnie bez potrzeby ręcznego wpisywania klucza licencyjnego. Oferowany dostarczony system jak i również jego

		reinstalacja nie może wymagać aktywacji klucza licencyjnego za pośrednictwem telefonu i Internetu; • Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim;
17.	Oprogramowanie dodatkowe	• Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci; • System Diagnostyczny działający nawet w przypadku uszkodzenia dysku twardego z systemem operacyjnym komputera.
18.	Bezpieczeństwo	• Moduł TPM lub równoważny.
19.	BIOS	• BIOS zgodny ze specyfikacją UEFI; • Możliwość odczytania z BIOS bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych następujących informacji: - Wersji BIOS, - Nr seryjnym komputera, - Ilości pamięci RAM, - Typie procesora i jego prędkości, - Modele zainstalowanych dysków twardych.
20.	Certyfikaty i standardy	• Deklaracja zgodności CE (załączyć do oferty); • Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS (załączyć do ofert); • Potwierdzenie poprawnej współpracy komputera z systemem operacyjnym - Wykonawca dołączy do oferty dokument w postaci wydruku potwierdzający certyfikację.
21.	Waga	• Waga urządzenia z baterią podstawową nie większa niż 1,8 kg.
22.	Gwarancja	• Co najmniej 36-miesięczna gwarancja producenta, świadczona w siedzibie Zamawiającego na miejscu u, w przypadku gdy konieczna będzie naprawa sprzętu w siedzibie producenta lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu pokrywa Wykonawca, • W przypadku wymiany dysku twardego uszkodzony dysk pozostaje u Zamawiającego, klienta; • Karta gwarancyjna producenta i warunki gwarancji dostarczone wraz ze sprzętem, obejmujące wszystkie opcje serwisowe wymagane przez Zamawiającego; • Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
23.	Wyposażenie dodatkowe	• Torba do laptopa dopasowana do jego wielkości, kolor czarny, granatowy, ciemny szary lub szary; • Mysz zewnętrzna, przewodowa, usb, standardowa: 2 przyciski+scroll.
24.	Wymagania dodatkowe	• Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu.

3.3.3 Telefon stacjonarny VOIP – 12 szt.

Lp.	Nazwa komponentu	Wymagane parametry techniczne urządzenia
1	Typ	• Przewodowy telefon stacjonarny dedykowany do pracy w sieci VOIP Starostwa Powiatowego w Kielcach. Proponowany kompatybilny model to: **Siemens/ Unify OpenStage 15 HFA (L30250-F600-C179)** lub równoważny o identycznych parametrach. Wymagana pełna kompatybilność z istniejącym typem centrali telefonicznej.
2	Złącza	• Min.: 2x RJ 45 (min 1 x 1 Gbs), 1xRJ 11.
3	Obudowa	• Plastikowa, połączona z plastikową słuchawką za pomocą przewodu RJ11; • Wbudowany wyświetlacz monochromatyczny o rozdzielczości min.: 205 x 41 pikseli, min. 2 wiersze; • Wbudowany czujnik odłożenia słuchawki; • Kolor obudowy – biały, srebrny, szary lub czarny, grafit; • Wbudowany switch min. 1 GB/s; • Możliwość zawieszenia pionowego np. na ścianie.
4	Funkcje dodatkowe	• Stałe przyciski funkcyjne, częściowo podświetlane; • Regulacja głośności za pomocą przycisków; • Możliwość odbierania rozmowy w trybie głośnomówiącym; • Wbudowane przyciski, pod którymi można zapisac na stałe w pamięci numer telefonu, tzw „stały kontakt" min. 7 szt; • Funkcja udostępnienia sieci LAN za pomocą przewodu do

		komputera; • Wydzielone przyciski nawigacyjne; • Możliwość wyboru rodzaju oraz tonu dzwonka; • Współpraca z oprogramowaniem do zarządzania połączeniami z poziomu aplikacji pracującej na Windows 7/10.
5	Wymiary (WxSxG), z połążoną słuchawką, bez opakowania	• Maks. 140mm x 300mm x 300mm.
6	Waga	• Maks. 1 kg.
7	Gwarancja	• Na okres co najmniej 12 miesięcy - świadczonej w siedzibie Zamawiającego, chyba że niezbędna będzie naprawa sprzętu w siedzibie producenta lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca; • Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
8	Wymagania dodatkowe	• Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu.

3.3.4 Drukarka przenośna, atramentowa – 1 szt.

Lp.	Nazwa komponentu	Wymagane parametry techniczne urządzenia
1	Typ	• Drukarka przenośna, atramentowa, A4, akumulatorowo – sieciowa.
2	Rozdzielczość drukowania	• Min: 4800x1200 dpi.
3	Szybkość drukowania	• W trybie monochromatycznym min: 8 obraz/minutę • w kolorze min: 5 obraz/minutę.
4	Drukowanie dwustronne	• obsługa ręczna.
5	Podajnik arkuszy:	• min. 50 arkuszy.
6	Obsługiwane formaty papieru:	• A4, A5, B5, DL (długość DIN), Legal, Letter, 10x15 cm.
7	Komunikacja	• Min: USB x1; • WiFi: min: IEEE802.11 b/g/n.

8	Wyświetlacz	• Typu OLED min: 3,6 cm (1,44"), monochromatyczny.
9	Wymiary	• Szerokość maks: 35 cm, Wysokość: 8 cm, Głębokość/Długość: 20 cm.
1	Waga	• Maks: 2,4 Kg.
1	Kolor	• Czarny, szary, lub ciemny szary, grafit.
1	Zasilanie sieciowe	• Od min: 100 – do maks: 240 V.
1	Obsługiwane systemy operacyjne	• Windows 7/8.1/10 32 i 64 bit.
1	Wyposażenie	• Akcesoria: zasilacz, startowe wkłady atramentowe, kabel USB, instrukcje; • Dołączone oprogramowanie zarządzające oraz sterowniki; • **Akumulator w zestawie.**
1	Gwarancja	• Na okres co najmniej 24 miesięcy - świadczonej w siedzibie Zamawiającego, chyba że niezbędna będzie naprawa sprzętu w siedzibie producenta lub autoryzowanym przez niego punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca; • Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
1	Wymagania dodatkowe	• Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu.

3.3.5 Pamięć RAM 16 GB dedykowana – 10 szt.

Lp.	Nazwa komponentu	Wymagane parametry techniczne urządzenia
17.	Typ	• DRAM, DDR 5, DIMM 288-pin dedykowana do Dell lub równoważna.
18.	Pojemność modułu	• Min. 16 GB.
19.	Szybkość	• Min. 4800 MHz (PC5-38400).
20.	Taktowanie	• Min. 2400 MHz.
21.	Korekcja błędów (ECC)	• Brak.
22.	Kompatybilność	• Pełna kompatybilność min. z modelem Dell Precision 3660 lub równoważnym.
23.	Gwarancja	• Na okres co najmniej 5 lat - świadczonej w siedzibie Zamawiającego, chyba że niezbędna będzie naprawa sprzętu w siedzibie producenta lub autoryzowanym przez niego

		punkcie serwisowym - wówczas koszt transportu do i z naprawy pokrywa Wykonawca; • Serwis urządzeń musi być realizowany przez Producenta lub Autoryzowanego Partnera Serwisowego Producenta.
24.	Wymagania dodatkowe	• Zamawiający zastrzega sobie prawo sprawdzenia pełnej zgodności parametrów oferowanego sprzętu.

4. Dostawa serwera plików wraz z dyskami.

4.1 Ilości.

SPRZĘT	ILOŚĆ
Dostawa serwera plików wraz z dyskami.	1 szt.

4.2 Postanowienia ogólne.

Opis przedmiotu zamówienia

Przedmiotem niniejszego zamówienia jest dostawa serwera plików wraz z dyskami w obudowie RACK na potrzeby Starostwa Powiatowego w Kielcach.

Dostawa urządzeń obejmuje wyspecyfikowane poniżej elementy.

Postępowanie prowadzone jest w formie zadania, którym jest dostawa wszystkich wymaganych przez Zamawiającego komponentów sprzętu komputerowego.

4.2.2 Serwer plików wraz z dyskami

	Nazwa komponentu	Wymagane parametry techniczne urządzenia
1.	Typ serwera plików	Serwer plików w obudowie RACK 2U
2.	Zainstalowana pamięć RAM	• Min. 64 GB, ECC, dedykowana do urządzenia • Obsługa min 64 GB ram
3.	Procesor	Dedykowany do tego typu urządzenia, wymagane min 4 rdzenie fizyczne, min. 8 wątków, z obsługą RAM ECC od min. 120 GB . Wymagana pamięć podręczna L3: min. 6 MB.
4.	Liczba obsługiwanych dysków	Min. 12 szt.
5.	Wielkość obsługiwanych dysków	• Zarówno 2,5 " jak i 3,5 ", HDD jak i SSD, • Możliwość wymiany dysku podczas pracy urządzenia (tzw:

	Nazwa komponentu	Wymagane parametry techniczne urządzenia
		hot-swap)
6.	Złącza	• Min. 4 x RJ 45, (z obsługą funkcji Link Aggregation / przełączania awaryjnego), • Min. 2 x USB 3.0 • Złącze zasilania sieciowego • Wewnątrz: min. 4 x pamięć RAM
7.	Obsługiwane typy RAID	• Min.: 0, 1, 5, 6, 10, F1, JBOD
8.	Funkcje	• AFP, • CalDAV, • Cloud Station, • iSCSI, • LDAP, • Ochrona antywirusowa, • Serwer: CIFS, DLNA, FTP (SSL/TLS), NFS, mail, SQL, VPN, SHA, SNMP, SSH, Telnet, WebDAV, Windows AD
9.	Zarządzanie serwerem	• Zarządzanie przez WWW.
10.	Wymagane obsługiwane systemy plików	• Btrfs • EXT4 • EXT3 • FAT • NTFS • HFS+
11.	Waga	Maks: 15 Kg
12.	Wyposażenie	• dołączony zestaw szyn montażowych • dołączone dedykowane dyski HDD 3,5 " o pojemności 10 TB każdy, z przeznaczeniem do NAS – 12 szt.
13.	Certyfikaty	Min: FCC, CE, BSMI, EAC, CCC, VCCI, RCM, RoHS
14.	Gwarancja i wsparcie	• 5 - letni okres gwarancji na urządzenie; • Min. 12 miesięcy na dyski twarde z opcją pozostawienia u Zamawiającego w razie awarii. • Realizowana w miejscu instalacji sprzętu, gwarantowana wizyta certyfikowanego serwisanta producenta w miejscu użytkowania sprzętu do końca następnego dnia roboczego od zgłoszenia; • Firma serwisująca musi posiadać ISO 9001:2000 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta – dokumenty potwierdzające załączyć do oferty.

5. Dostawa licencji oprogramowania systemu antywirusowego na 375 stanowisk.

5.1 Ilości.

SPRZĘT	ILOŚĆ
Dostawa licencji oprogramowania systemu antywirusowego na 375 stanowisk.	1 szt.

5.2 Postanowienia ogólne.

Opis przedmiotu zamówienia

Dostawa licencji oprogramowania systemu antywirusowego dla Starostwa Powiatowego w Kielcach na 375 stanowisk na okres ochrony 36 miesięcy

Zakup licencji systemu ochrony antywirusowej zapewniającej ochronę:

- **antywirusową i antyspyware'ową serwerów oraz stacji roboczych z rodziny Windows oraz Linux – łącznie 375 sztuk,**
- **antywirusową, antyspyware'ową oraz antyspamową serwerów pocztowych MS Exchange w wersjach co najmniej 2007-2016,**
- **antywirusową i antyspyware'ową fizycznych serwerów ESXi oraz znajdujących się na nich maszyn wirtualnych – ochrona bezagentowa środowiska VMware**

np. ESET Secure Business AV LEVEL wraz z 36 miesięcznym wsparciem lub dostawa licencji równoważnego systemu ochrony antywirusowej wraz z 36 miesięcznym wsparciem.

Równoważność oznacza że:

1) produkt równoważny musi być kompatybilny i w sposób niezakłócony współdziałać ze sprzętem i oprogramowaniem posiadanym przez Zamawiającego,
2) produkt równoważny musi w pełni współpracować z systemami zarówno 32 jak i 64 bitowymi,
3) produkt równoważny musi w pełni współpracować z oprogramowaniem zainstalowanym na:

a) Systemy Windows w tym: Windows 7/Windows 8/Windows 8.1/Windows 8.1 Update /Windows 10/ Windows 11 oraz Microsoft Windows Server 2012, 2012 R2, 2016 R2
b) Systemy Apple Mac OS X,
c) Systemy Linux w tym: dla dystrybucji Red Hat Mandriva, Suse oraz innych z nimi zgodnych, dla dystrybucji Debian, Ubuntu, CentOS oraz innych z nimi zgodnych, systemów FreeBSD 5.x, 6.x i 7.x oraz systemów NetBSD oraz Solaris

d) Urządzeniach przenośnych/smartfonach - Symbian i Windows Mobile,

e) Urządzeniach przenośnych/smartfonach Android w tym: co najmniej Android 2.0,

4) Pomoc w programie (help) i dokumentacja do programu w języku polskim.

Ochrona antywirusowa i antyspyware

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
3. Wbudowana technologia do ochrony przed rootkitami.
4. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
7. System ma oferować administratorowi możliwość definiowania zadań w harmonogramie w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym i jeśli tak – nie wykonywało danego zadania.
8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
9. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu.
11. Możliwość skanowania dysków sieciowych i dysków przenośnych.
12. Skanowanie plików spakowanych i skompresowanych.
13. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
14. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
15. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
16. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 min lub do ponownego uruchomienia komputera.
17. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
18. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
19. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
20. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
21. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

22. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
23. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
24. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
25. Blokowanie możliwości przeglądania wybranych stron internetowych. Listę blokowanych stron internetowych określa administrator. Program musi umożliwić blokowanie danej strony internetowej po podaniu na liście całej nazwy strony lub tylko wybranego słowa występującego w nazwie strony.
26. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron ustalonej przez administratora.
27. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
28. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
29. Program ma zapewniać skanowanie ruchu HTTPS transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji takich jak przeglądarki Web lub programy pocztowe.
30. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika w celu analizy przez laboratorium producenta.
31. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
32. Program musi posiadać funkcjonalność która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
33. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania na żądanie oraz przez moduły ochrony w czasie rzeczywistym.
34. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
35. W przypadku gdy stacja robocza nie będzie posiadała dostępu do sieci Internet ma odbywać się skanowanie wszystkich procesów również tych, które wcześniej zostały uznane za bezpieczne.
36. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka).
37. Do wysłania próbki zagrożenia do laboratorium producenta aplikacja nie może wykorzystywać klienta pocztowego wykorzystywanego na komputerze użytkownika.
38. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
39. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
40. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
41. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy komputerze przy próbie dostępu do konfiguracji był proszony o podanie hasła.
42. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.

43. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji powinno być takie samo.
44. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.
45. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
46. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
47. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
48. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
49. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM , urządzeń przenośnych oraz urządzeń dowolnego typu.
50. Funkcja blokowania nośników wymiennych bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia, model.
51. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia, dana funkcjonalność musi pozwalać na automatyczne wypełnienie właściwości urządzenia dla tworzonej reguły.
52. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie brak dostępu do podłączanego urządzenia.
53. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
54. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
55. Użytkownik ma posiadać możliwość takiej konfiguracji programu aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika
56. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
57. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:

- tryb automatyczny z regułami gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
- tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
- tryb oparty na regułach gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
- tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach.

- Tryb inteligentny – w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.

58. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
59. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
60. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
61. Program musi być wyposażona w mechanizm ochrony przed exploitami w popularnych aplikacjach np. czytnikach PDF, aplikacjach JAVA itp.
62. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
63. Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
64. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.
65. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
66. Możliwość określenia maksymalnego czasu ważności dla bazy danych sygnatur, po upływie czasu i braku aktualizacji program zgłosi posiadanie nieaktualnej bazy sygnatur.
67. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji.
68. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji za pomocą wbudowanego w program serwera http.
69. Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (rollback).
70. Program powinien być wyposażony tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
71. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełno ekranowym.
72. W momencie wykrycia trybu pełno ekranowego aplikacja ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań aplikacji.
73. Użytkownik ma mieć możliwość skonfigurowania programu tak aby automatycznie program włączał powiadomienia oraz zadania pomimo pracy w trybie pełnoekranowym po określonym przez użytkownika czasie.
74. Program ma być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, modułu antyspamowego, kontroli stron Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.
75. Wsparcie techniczne do programu świadczone w języku polskim przez podmiot autoryzowany przez producenta programu.
76. Program musi posiadać możliwość utworzenia z poziomu interfejsu aplikacji dziennika diagnostycznego na potrzeby pomocy technicznej.

77. Program musi posiadać możliwość aktywacji poprzez podanie konta administratora licencji, podanie klucza licencyjnego oraz możliwość aktywacji programu offline.
78. Możliwość podejrzenia licencji za pomocą której program został aktywowany.

Ochrona serwera plików Windows

1. Wsparcie dla systemów: Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016, SBS 2003, SBS 2003 R2, SBS 2008, SBS 2011, Microsoft MultiPoint Server 2010, Microsoft MultiPoint Server 2011, Windows MultiPoint Server 2012.
2. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
3. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor, itp.
4. Wbudowana technologia do ochrony przed rootkitami i exploitami.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
7. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
8. Skanowanie "na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
9. System antywirusowy ma mieć możliwość określania poziomu obciążenia procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu.
10. System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
11. Użytkownik ma mieć możliwość zmiany ilości wątków skanowania w ustawieniach systemu antywirusowego.
12. Możliwość skanowania dysków sieciowych i dysków przenośnych.
13. Skanowanie plików spakowanych i skompresowanych.
14. Możliwość umieszczenia na liście wyłączeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
15. Program musi posiadać funkcjonalność pozwalającą na ograniczenie wielokrotnego skanowania plików w środowisku wirtualnym za pomocą mechanizmu przechowującego informacje o przeskanowanym już obiekcie i współdzieleniu tych informacji z innymi maszynami wirtualnymi.
16. Aplikacja powinna wspierać mechanizm klastrowania.
17. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
18. Program powinien oferować możliwość skanowania dysków sieciowych typu NAS.
19. Aplikacja musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
20. Program ma umożliwiać użytkownikowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, płyt CD/DVD i pamięci masowych FireWire.
21. Funkcja blokowania nośników wymiennych ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ urządzenia, numer seryjny urządzenia, dostawcę urządzenia.
22. Aplikacja musi posiadać funkcjonalność, która automatycznie uzupełni elementy wymagane dla tworzenia reguł w oparciu o informacje dostępne z aktualnie podłączonego nośnika.
23. Aplikacja ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, brak dostępu do podłączanego urządzenia.

24. Aplikacja ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
25. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
26. System antywirusowy ma automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
27. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
28. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
29. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
30. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
31. W przypadku restartu serwera – usunięte z listy wyłączeń elementy mają być automatycznie uzupełnione.
32. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji systemu antywirusowego.
33. System antywirusowy ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
34. Możliwość przeniesienia zainfekowanych plików w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
35. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka).
36. Możliwość skanowania wyłącznie z zastosowaniem algorytmów heurystycznych tj. wyłączenie skanowania przy pomocy sygnatur baz wirusów.
37. Aktualizacje modułów analizy heurystycznej.
38. Możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
39. Wysyłanie zagrożeń do laboratorium ma być możliwe z serwera zdalnego zarządzania i lokalnie z każdej stacji roboczej w przypadku komputerów mobilnych.
40. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
41. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
42. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
43. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby użytkownik siedzący przy serwerze przy próbie dostępu do konfiguracji systemu antywirusowego był proszony o podanie hasła.
44. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.
45. Hasło do zabezpieczenia konfiguracji programu oraz jego nieautoryzowanej próby, deinstalacji ma być takie samo.
46. System antywirusowy ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika wraz z listą niezainstalowanych aktualizacji.
47. System antywirusowy ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne,

aktualizacje ważne, aktualizacje zwykle oraz aktualizacje o niskim priorytecie. Program ma także posiadać opcję dezaktywacji tego mechanizmu.

48. Po instalacji systemu antywirusowego, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu wirusów.
49. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma umożliwiać pełną aktualizację baz sygnatur wirusów z Internetu lub z bazy zapisanej na dysku.
50. System antywirusowy uruchomiony z płyty bootowalnej lub pamięci USB ma pracować w trybie graficznym.
51. Program powinien umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: nośników CD/DVD oraz urządzeń USB.
52. System antywirusowy ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesach i połączeniach.
53. System antywirusowy ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.
54. Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń.
55. Aktualizacja dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD, DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
56. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
57. Możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja).
58. Do każdego zadania aktualizacji można przypisać dwa różne profile z innym ustawieniami (serwer aktualizacyjny, ustawienia sieci, autoryzacja). Przykładowo, domyślny profil aktualizuje z sieci lokalnej a w przypadku jego niedostępności wybierany jest profil rezerwowy pobierający aktualizację z Internetu.
59. System antywirusowy wyposażony w tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
60. Aplikacja musi wspierać skanowanie magazynu Hyper-V.
61. Aplikacja musi posiadać możliwość wykluczania ze skanowania procesów.
62. Praca programu musi być niezauważalna dla użytkownika.
63. Dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji baz wirusów i samego oprogramowania.
64. Wsparcie techniczne do programu świadczone w języku polskim przez podmiot autoryzowany przez producenta programu.

Administracja zdalna

1. Serwer administracyjny musi oferować możliwość instalacji na systemach Windows Server od 2012 oraz systemach Linux.
2. Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) lub dysku wirtualnego w formacie VHD.
3. Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL.
4. Serwer administracyjny musi oferować możliwość wykorzystania już istniejącej bazy danych MS SQL lub MySQL użytkownika.

5. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji i konsoli w postaci jednego pakietu instalacyjnego lub każdego z modułów oddzielnie bezpośrednio ze strony producenta.
6. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW niezależnie od platformy sprzętowej i programowej.
7. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.
8. Narzędzie musi być kompatybilne z protokołami IPv4 oraz IPv6.
9. Podczas logowania administrator musi mieć możliwość wyboru języka w jakim zostanie wyświetlony panel zarządzający.
10. Zmiana języka panelu administracyjnego nie może wymagać zatrzymania lub reinstalacji oprogramowania zarządzającego.
11. Komunikacja z konsolą powinna być zabezpieczona się za pośrednictwem protokołu SSL.
12. Narzędzie do administracji zdalnej musi posiadać moduł pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
13. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
14. Jeden centralny serwer centralnego zarządzania bez względu na wielkość sieci.
15. Instalacja serwera administracyjnego powinna oferować wybór trybu pracy serwera w sieci w przypadku rozproszonych sieci –serwer pośredniczący (proxy) lub serwer centralny.
16. Serwer proxy musi pełnić funkcję pośrednika pomiędzy lokalizacjami zdalnymi a serwerem centralnym.
17. Serwer proxy musi być wyposażony we własną bazę danych, w której będą przechowywane dane z agentów na wypadek braku połączenia z serwerem centralnym.
18. Serwer administracyjny musi oferować możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
19. Serwer administracyjny musi oferować możliwość instalacji serwera http proxy pozwalającego na pobieranie aktualizacji baz sygnatur oraz pakietów instalacyjnych na stacjach roboczych bez dostępu do Internetu.
20. Serwer http proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) najczęściej pobieranych elementów.
21. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
22. Serwer administracyjny musi oferować możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy.
23. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na stacjach roboczych z systemami Windows, Mac OS X oraz Linux oraz serwerach Windows.
24. Centralna administracja musi pozwalać na zarządzanie programami zabezpieczającymi na urządzeniach mobilnych z systemem Android.
25. Centralna konfiguracja i zarządzanie ochroną antywirusową, antyspyware'ową i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
26. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
27. Administrator musi posiadać możliwość zarządzania za pomocą dedykowanego agenta stacjami nie posiadającymi zainstalowanego programu zabezpieczającego.
28. Agent musi przekazywać informacje na temat stanu systemu operacyjnego do serwera administracji zdalnej.
29. Agent musi posiadać możliwość pobrania listy zainstalowanego oprogramowania firm trzecich na stacji roboczej z możliwością jego odinstalowania.
30. Serwer administracyjny musi oferować możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.

31. Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego.
32. Instalacja agenta nie może wymagać określenia typu systemu (32 lub 64 – bitowy) oraz jego rodzaju (Windows, Mac, itp) a dobór odpowiedniego pakietu musi być w pełni automatyczny.
33. Instalacja klienta na urządzeniach mobilnych musi być dostępna za pośrednictwem portalu WWW udostępnionego przez moduł MDM z poziomu urządzenia użytkownika.
34. W przypadku braku zainstalowanego klienta na urządzeniu mobilnym musi istnieć możliwość jego pobrania ze sklepu Google Play.
35. Administrator musi posiadać możliwość utworzenia listy zautoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
36. Serwer administracyjny musi oferować możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, nie komunikację za pośrednictwem wiadomości SMS.
37. Serwer administracyjny musi oferować możliwość utworzenia polityk konfiguracji dla aplikacji zabezpieczającej na urządzeniu mobilnym.
38. Administrator musi posiadać możliwość utworzenia dodatkowych użytkowników/administratorów Serwer centralnego zarządzania do zarządzania stacjami roboczymi.
39. Administrator powinien posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli zarządzającej
40. Dwu fazowa autoryzacja musi się odbywać za pomocą wiadomości SMS lub haseł jednorazowych generowanych na urządzeniu mobilnym za pomocą dedykowanej aplikacji.
41. Administrator musi posiadać możliwość utworzenia użytkownika wbudowanego lub zintegrowanego z grupą z usługi Active Directory.
42. Serwer administracyjny musi oferować możliwość utworzenia zestawów uprawnień dotyczących zarządzania poszczególnymi grupami komputerów, politykami, instalacją agenta, raportowania, zarządzania licencjami, zadaniami, itp.
43. Administrator musi posiadać możliwość nadania dwóch typów uprawnień do każdej z funkcji przypisanej w zestawie uprawnień: tylko do odczytu, odczyt/zapis.
44. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
45. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta bez konieczności logowania się do panelu administracyjnego.
46. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności po jakim użytkownik zostanie automatycznie wylogowany.
47. Dostępne zadania muszą być podzielone na dwie grupy: zadania klienta oraz zadania serwera.
48. Zadania serwera obejmujące zadanie instalacji agenta, generowania raportów oraz synchronizacji grup.
49. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
50. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
51. Serwer administracyjny musi w przejrzysty sposób informować administratora o elementach zadań jakie są wymagane do jego uruchomienia a w przypadku jego braku wskazywać brakujące elementy konfiguracji.
52. Instalacja zdalna programu zabezpieczającego za pośrednictwem agenta musi odbywać się z repozytorium producenta lub z pakietu dostępnego w Internecie lub zasobie lokalnym.
53. Serwer administracyjny musi oferować możliwość wyboru parametrów pakietu instalacyjnego zależnych od systemu operacyjnego oraz licencji na program zabezpieczający.

54. Serwer administracyjny musi oferować możliwość deinstalacji programu zabezpieczającego firm trzecich lub jego niepełnej instalacji podczas instalacji nowego pakietu.
55. Serwer administracyjny musi oferować możliwość wysłania komunikatu lub polecenia na stacje kliencką.
56. Serwer administracyjny musi oferować możliwość utworzenia jednego zadania dla kilku klientów lub grupy.
57. Serwer administracyjny musi oferować możliwość uruchomienia zadania automatycznie zgodnie z harmonogramem, po wystąpieniu nowego dziennika zdarzeń lub umieszczeniu nowego klienta w grupie dynamicznej.
58. Serwer administracyjny musi oferować możliwość utworzenia grup statycznych i dynamicznych komputerów.
59. Grupy dynamiczne tworzone na podstawie szablonu określającego warunki jakie musi spełnić klient aby zostać umieszczony w danej grupie. Przykładowe warunki: Adresy sieciowe IP, Aktywne zagrożenia, Stan funkcjonowania/ochrony, Wersja systemu operacyjnego, itp.
60. Serwer administracyjny musi oferować możliwość utworzenia polityk dla programów zabezpieczających i modułów serwera centralnego zarządzania.
61. Serwer administracyjny musi oferować możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów. Serwer administracyjny musi oferować możliwość przypisania kilku polityk z innymi priorytetami dla jednego klienta.
62. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień zaawansowanych w programie zabezpieczającym na stacji roboczej.
63. Serwer administracyjny musi oferować możliwość nadania priorytetu „Wymuś" dla konkretnej opcji w konfiguracji klienta. Opcja ta nie będzie mogła być zmieniona na stacji klienckiej bez względu na zabezpieczenie całej konfiguracji hasłem lub w przypadku jego braku.
64. Serwer administracyjny musi oferować możliwość ukrycia graficznego interfejsu użytkownika na stacji klienckiej i jego uruchomienia tylko przez administratora.
65. Serwer administracyjny musi umożliwiać wyświetlenie polityk do których przynależy dana stacja robocza oraz ich edycję z poziomu właściwości samego klienta
66. Serwer administracyjny musi oferować możliwość utworzenia własnych raportów lub skorzystanie z predefiniowanych wzorów.
67. Serwer administracyjny musi oferować możliwość utworzenia raportów zawierających dane zebrane przez agenta ze stacji roboczej i serwer centralnego zarządzania.
68. Serwer administracyjny musi oferować możliwość wyboru formy przedstawienia danych w raporcie w postaci tabeli, wykresu lub obu elementów jednocześnie.
69. Serwer administracyjny musi oferować możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy, itp.
70. Serwer administracyjny musi oferować możliwość określenia danych jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na elementach wykresu oraz ich odfiltrowania i posortowania.
71. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
72. Serwer administracyjny powinien posiadać Panel kontrolny z raportami administratora, pozwalający na szybki dostępu do najbardziej interesujących go danych. Panel ten musi oferować możliwość modyfikacji jego elementów.
73. Serwer administracyjny musi oferować możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenie raportu na Panelu kontrolnym dostępnym z poziomu interfejsu konsoli WWW.
74. Raport generowany okresowo może zostać wysłany za pośrednictwem wiadomości email lub zapisany do pliku w formacie PDF, CSV lub PS.
75. Serwer administracyjny musi oferować możliwość skonfigurowania czasu automatycznego odświeżania raportu na panelu kontrolnym oraz umożliwiać jego odświeżenie na żądanie.

76. Serwer administracyjny musi oferować możliwość tworzenia wielu zakładek panelu, w których będą widoczne wybrane przez administratora elementy monitorujące.
77. Serwer administracyjny musi oferować możliwość maksymalizacji wybranego elementu monitorującego.
78. Raport na panelu kontrolnym musi być w pełni interaktywny pozwalając przejść do zarządzania stacjom/stacjami, której raport dotyczy.
79. Serwer administracyjny musi oferować możliwość utworzenia własnych powiadomień lub skorzystanie z predefiniowanych wzorów.
80. Powiadomienia muszą dotyczyć zmiany ilości klientów danej grupy dynamicznej, wzrostu liczby grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń lub skanowania lub stanu obiektu serwer centralnego zarządzania.
81. Administrator musi posiadać możliwość wysłania powiadomienia za pośrednictwem wiadomości email lub komunikatu SNMP.
82. Serwer administracyjny musi oferować możliwość konfiguracji własnej treści komunikatu w powiadomieniu.
83. Serwer administracyjny musi oferować możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
84. Serwer administracyjny musi oferować możliwość dodania licencji do serwera zarządzania na podstawie klucza licencyjnego lub pliku offline licencji.
85. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji obejmujących różne produkty.
86. Serwer administracyjny musi oferować możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
87. Narzędzie administracyjne musi być wyposażone w mechanizm wyszukiwania zarządzanych komputerów na podstawie co najmniej nazwy komputera, adresu IPv4 i IPv6 lub wyszukania konkretnej nazwy zagrożenia.

Ochrona poczty MS Exchange

1. Musi zapewniać wsparcie dla systemów poczty Microsoft Exchange 2007/2010/2013/2016
2. Musi zapewniać wsparcie dla ról Mailbox, Edge, Hub, Client Access Server
3. Aplikacja musi umożliwiać Administratorowi na etapie instalacji wybór komponentów jakie mają być zainstalowane.
4. Aplikacja musi skanować pocztę przychodzącą i wychodzącą na serwerze MS Exchange.
5. Program ma zapewnić skanowanie bezpośrednio w storach Exchange przy pomocy VSAPI.
6. Program musi mieć możliwość zdefiniowania kilku wątków skanujących w celu optymalizacji pracy serwera.
7. Program ma zapewnić skanowanie przed zapisaniem wiadomości w storze przy pomocy transport agenta.
8. W przypadku wykrycia wirusa/blokowania wiadomości system musi umożliwić usunięcie wiadomości/ załącznika, podmianę załącznika na czysty plik zawierający jedynie informację o infekcji.
9. Możliwość tworzenia różnych reguł blokowania wiadomości w tym co najmniej po zdefiniowanym nadawcy, odbiorcy, temacie wiadomości, typie załącznika, rozmiarze załącznika, rozmiarze wiadomości, nagłówku wiadomości, na podstawie uzyskanego wyniku skanowania antyspamowego i antywirusowego, godzinie odbioru, obecności załącznika chronionego hasłem lub uszkodzonego archiwum.
10. Program musi posiadać możliwość tworzenia białych i czarnych list domen/adresów IP, adresów e-mail.

11. Aplikacja musi posiadać możliwość akceptacji białych list stworzonych na poziomie serwera MS Exchange.
12. Program musi posiadać wbudowany w oprogramowanie filtr antyspamowy odpowiedzialny za filtrowanie niechcianej poczty.
13. System antyspamowy ma być wyposażony przynajmniej w możliwość sprawdzania list RBL, DNSBL oraz mechanizm reputacji poczty.
14. Administrator musi mieć możliwość dodania własnych adresów list RBL oraz DSBL z których będzie korzystać aplikacja.
15. Program ma posiadać mechanizmy greylistingu (szare listy).
16. Aplikacja musi posiadać możliwość tworzenia wyjątków dla mechanizmu greylistingu.
17. Program ma posiadać możliwość stworzenia End User Quarantine.
18. Kwarantanna musi być dostępna dla użytkownika końcowego za pośrednictwem przeglądarki www.
19. Użytkownik końcowy musi posiadać możliwość zarządzania wiadomościami znajdującymi się w kwarantannie w tym co najmniej, mieć możliwość uwolnienia wiadomości z kwarantanny, jej usunięcia lub pozostawienia w kwarantannie.
20. Administrator musi mieć możliwość wglądu w globalną kwarantannę z poziomu interfejsu aplikacji oraz przeglądarki www.
21. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików serwera "na żądanie" lub według harmonogramu.
22. Wykrywanie niebezpiecznych aplikacji typu Adware, Spyware, Dialer itp.
23. Wbudowana technologia do ochrony przed rootkitami.
24. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
25. Skanowanie plików spakowanych i skompresowanych.
26. Aplikacja musi w momencie instalacji na serwerze wykrywać usługi jakie są zainstalowane i tworzyć odpowiednie wyjątki dla nich.
27. Aplikacja musi być wyposażona w mechanizm chroniący serwer przed exploitami i atakami typu 0-day.
28. Aplikacja musi posiadać zaawansowany skaner pamięci umożliwiający wykrywanie zagrożeń próbujących działać na poziomie pamięci operacyjnej serwera.
29. Zainstalowany system ochrony musi być wyposażony w system HIPS.
30. Aplikacja musi w natywny sposób wspierać środowiska klastrowe.
31. System musi umożliwiać wskazanie zewnętrznych lokalizacji w których przechowywane będą moduły i aktualizacje programu.
32. Aplikacja musi wspierać WMI za pomocą których może przekazywać podstawowe informacje na temat swojej pracy do zewnętrznych systemów np. SIEM.
33. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail, Windows Live Mail zainstalowanego lokalnie na serwerze pocztowym.
34. Możliwość utworzenia kilku zadań skanowania (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami (metody skanowania, obiekty skanowania, czynności) .
35. Pliki zapisywane w katalogu kwarantanny powinny być szyfrowane.
36. Aplikacja musi umożliwiać aktualizację modułów ochrony bez konieczności re instalacji całego programu.
37. Aplikacja musi być wyposażona w dwa niezależnie pracujące mechanizmy analizy heurystycznej (standardowa i zaawansowana heurystyka).
38. Aplikacja musi umożliwiać automatyczne wysyłanie nowych zagrożeń (wykrytych przez heurystykę) do laboratorium producenta przez program antywirusowy – nie wymaga ingerencji użytkownika.
39. Wysyłanie nowych zagrożeń musi być możliwe za pomocą interfejsu aplikacji i nie może do tego celu wykorzystywać klienta pocztowego zainstalowanego w systemie.

40. Program musi umożliwiać wysyłanie wraz z próbką adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
41. W przypadku wykrycia wirusa, ostrzeżenie może zostać wysłane do administratora poprzez e-mail.
42. Aplikacja musi posiadać wbudowany dziennik zdarzeń rejestrujący informacje na temat znalezionych wirusów, dokonanych aktualizacji baz wirusów i wersji oprogramowania.
43. Administrator musi mieć możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu.
44. Możliwość zabezpieczenia hasłem musi obejmować wyłączenie programu antywirusowego oraz jego odinstalowanie.
45. Aplikacja musi w sposób automatyczny i przyrostowy dokonywać aktualizacji baz sygnatur wirusów.
46. Aktualizacja musi być dostępna z Internetu, lokalnego zasobu sieciowego, nośnika CD/DVD lub napędu USB, a także przy pomocy protokołu HTTP z dowolnej stacji roboczej lub serwera (program antywirusowy z wbudowanym serwerem HTTP).
47. Aplikacja musi posiadać możliwość automatycznego ściągania oraz udostępniania zbiorów aktualizacyjnych
48. Aplikacja musi wspierać aktualizacje za pośrednictwem serwera Proxy.
49. Administrator musi posiadać możliwość utworzenia kilku zadań aktualizacji (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z własnymi ustawieniami.
50. Program musi uruchamiać jeden skaner uruchamiany w pamięci, do którego odnoszą się wszystkie monitory skanujące i skanery na żądanie.
51. Aplikacja musi posiadać możliwość zdalnej administracji za pomocą konsoli administracji zdalnej.
52. Aplikacja musi posiadać wbudowany, dedykowany moduł command line umożliwiający konfigurację oraz uruchamianie zadań zainstalowanej aplikacji.
53. Aplikacja musi być wyposażona w narzędzie umożliwiające wygenerowanie raportu dotyczącego stanu komputera, w tym co najmniej zainstalowanych aplikacji, uruchomionych procesów, ważnych wpisów w rejestrze i uruchomionych usług.
54. Do administracji zdalnej musi być wykorzystywany dedykowany agent.
55. Agent musi komunikować się z serwerem administracji zdalnej w bezpieczny sposób uniemożliwiający podsłuch komunikacji.
56. Skuteczność programu ma być potwierdzona nagrodami niezależnych organizacji (np. VB100, ISCA labs, Check Mark).
57. Wsparcie techniczne do programu świadczone w języku polskim przez podmiot autoryzowany przez producenta programu.

Ochrona środowiska wirtualnego VMware

1. Rozwiązanie zapewnia bezagentową ochronę maszyn wirtualnych w wersjach systemu gościa: Windows Vista x32, Windows 7 x32/x64, Windows Server 2008 x32/x64, Windows Server 2008 R2 x32/x64, Windows Server 2012 R2, Windows 8 x32/x64, Windows 8.1, Windows 10
2. Rozwiązanie umożliwia ochronę minimum 100 wirtualnych serwerów.
3. Ochrona środowiska wirtualnego zarządzana z jednej, centralnej konsoli administracyjnej, niezależnie od ilości chronionych hostów wirtualnych i serwerów w roli hypervisora.
4. W ramach całego chronionego środowiska wirtualnego wymagane jest uruchomienie tylko jednej maszyny wirtualnego hosta agenta.
5. Wyłączenie serwera z centralną konsolą administracyjną nie wpływa na działanie mechanizmów ochrony maszyn wirtualnych (silniki antywirusowe pozostają aktywne).

6. Wdrożenie rozwiązania do ochrony środowiska wirtualnego może być przeprowadzone w sposób zautomatyzowany z wykorzystaniem dedykowanego narzędzia, niezależnie od liczby serwerów wirtualnych.
7. Wdrożenie rozwiązania nie wymaga instalowania jakichkolwiek zewnętrznych składników czy plug-inów na natywnym systemie operacyjnym nadzorcy wirtualnego (hypervisora)
8. Rozwiązanie funkcjonuje bez konieczności instalowania jakiegokolwiek własnego agenta na systemach operacyjnych wirtualnych hostów
9. Rozwiązanie wspiera środowisko VMware vSphere 5.5 lub nowsze wraz z VMWare vShield.
10. Ochrona środowiska wirtualnego realizowana jest z wykorzystaniem VMWare vShield API.
11. Ochrona środowiska wirtualnego dostarczana jest wyłącznie w postaci obrazów maszyn wirtualnych (OVA- Open Virtual Appliance).
12. Rozwiązanie wspiera technologię Vmware vMotion Migration- host wirtualny jest chroniony w trybie ciągłym niezależnie od tego na jakim serwerze fizycznym znajduje się w ramach jednego środowiska vSphere.
13. System ochrony maszyny wirtualnej działa w trybie aktywnym (ochrona systemu w czasie rzeczywistym) jak i pasywnym (realizowanie skanowania 'na żądanie').
14. Mechanizmy ochrony wirtualnych serwerów i desktopów realizowane są bezagentowo przez sinik producenta uruchomiony na dedykowanym wirtualnym appliance.
15. Aktualizacje baz sygnatur antywirusowych pobierane są wyłączenie przez sinik producenta uruchomiony na dedykowanym wirtualnym appliance.
16. Silnik antywirusowy wykorzystuje mechanizmy weryfikowania w chmurze producenta plików i procesów w czasie rzeczywistym- musi istnieć możliwość zdecydowania, czy funkcja ta ma być włączona, czy też nie.
17. Do mechanizmów ochrony maszyn wirtualnych rozwiązanie wykorzystuje wyłączenie sieć zdefiniowaną programowo (SDN).
18. Wyłączenie adaptera sieci TCP/IP na maszynie wirtualnej w żaden sposób nie wpływa na jej ochronę przez silnik antywirusowy.

Stan aktualny

Zamawiający posiada wdrożony system ESET Secure Business AV LEVEL zapewniający ochronę łącznie 375 stacjom oraz serwerom.

Wdrożenie

Zamawiający uzna system za wdrożony, jeżeli wszystkie elementy systemu objęte dostawą zostaną prawidłowo uruchomione w infrastrukturze Zamawiającego, system zostanie zarejestrowany zgodnie z dostarczoną licencją i zostanie zauktualizowany do najnowszej wersji. System w dniu zakończenia wdrożenia musi zapewniać ochronę antywirusową/antyspyware'ową oraz antyspamową serwerom / stacjom roboczym Zamawiającego zgodnie z zakupioną licencją. Wdrożenie musi przeprowadzić certyfikowany inżynier dostarczonego w postepowaniu produktu.

Zamawiający w razie potrzeby udostępni połączenie zdalne w celu wykonania wdrożenia. Dostęp zdalny zostanie udostępniony na nadesłane żądanie Wykonawcy zawierające Imię i Nazwisko osoby uprawnionej, ze strony Wykonawcy, do wykonania prac u Zamawiającego oraz adres IP z którego połączenie będzie się odbywało. Wszelkie prace u Zamawiającego odbywają się pod nadzorem pracownika Zespołu ds. Informatyzacji Starostwa.

Zamawiający dopuszcza w postepowaniu, jako równoważne, oprogramowania posiadające:

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych programów: adware, spyware, scareware, phishing, hacktools itp.
3. Wbudowana technologia do ochrony przed rootkitami wykrywająca aktywne i nieaktywne rootkity.
4. Moduł do ochrony przed exploitami (ataki 0-day).
5. Moduł do ochrony przed ransomware.
6. Mechanizm ochrony przed zamaskowanym złośliwym kodem wykorzystujący sieć neuronową opartą o algorytmy adaptacyjne.
7. Klient oprogramowania antywirusowego dla stacji roboczych z systemami Linux.
8. Klient oprogramowania antywirusowego dla linuksowych serwerów Samba.
9. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
10. Dwa niezależne skanery antywirusowe (nie heurystyczne!) z dwoma niezależnymi bazami sygnatur wirusów wykorzystywane przez skaner dostępowy, skaner na żądanie oraz skaner poczty elektronicznej.
11. Możliwość konfiguracji programu do pracy z jednym skanerem i dwoma skanerami antywirusowymi jednocześnie.
12. Dodatkowy i niezależny od skanerów plików, trzeci skaner poczty oparty o technologię cloud security.
13. Możliwość wykluczenia ze skanowania skanera dostępowego: napędów, katalogów, plików lub procesów.
14. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików na żądanie lub według harmonogramu.
15. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rodzaj plików do skanowania, priorytet skanowania).
16. Skanowanie na żądanie pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
17. Technologia zapobiegająca powtórnemu skanowaniu sprawdzonych już plików, przy czym maksymalny czas od ostatniego sprawdzenia pliku nie może być dłuższy niż
4 tygodnie, niezależnie od tego czy plik był modyfikowany czy nie.
18. Możliwość określania poziomu obciążenia procesora podczas skanowania na żądanie i według harmonogramu.
19. Możliwość skanowania dysków sieciowych i dysków przenośnych.
20. Rozpoznawanie i skanowanie wszystkich znanych formatów kompresji.
21. Możliwość definiowania listy procesów, plików, folderów i napędów pomijanych przez skaner dostępowy.
22. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
23. Skanowanie i oczyszczanie poczty przychodzącej POP3 w czasie rzeczywistym, zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).

24. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
25. Możliwość definiowania różnych portów dla POP3, SMTP i IMAP na których ma odbywać się skanowanie.
26. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odebranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
27. Dodatek do aplikacji MS Outlook umożliwiający podejmowanie działań związanych z ochroną z poziomu programu pocztowego.
28. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
29. Dedykowany moduł chroniący przeglądarki przed szkodnikami atakującymi sesje z bankami i sklepami online.
30. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
31. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
32. Ochrona przed stronami phishingowymi działającymi przy użyciu protokołów HTTP
1 HTTPS.
33. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
34. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń powinny być w pełni anonimowe.
35. Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej.
36. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e mail.
37. Możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu.
38. Aktualizacja dostępna z bezpośrednio Internetu lub offline - z pliku pobranego zewnętrznie.
39. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
40. Możliwość określenia częstotliwości aktualizacji w odstępach 1 godzinowych.
41. Możliwość samodzielnej aktualizacji sygnatur wirusów ze stacji roboczej (np. komputery mobilne).
42. Program wyposażony w tylko w jeden serwer skanujący uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, skaner HTTP).
43. Możliwość ukrycia programu na stacji roboczej przed użytkownikiem.
44. Moduł ochrony proaktywnej, oparty na teorii grafów, uczący się zachowania systemu operacyjnego i wykrywający podejrzane działania.
45. Skanowanie w trybie bezczynności - pełne skanowanie komputera przynajmniej raz na
2 tygodnie uruchamiane i wznawiane automatycznie, podczas gdy nie jest on używany.
46. Ochrona przed urządzeniami podszywającymi się pod klawiatury USB.
47. Agentowa ochrona maszyn wirtualnych wykrywająca znane i nieznane zagrożenia przy użyciu zdalnego serwera skanowania oraz technologii proaktywnych.
48. Agent ochrony maszyn wirtualnych delegujący zlecenie skanowania do wirtualnego serwera skanowania.
49. Wirtualny serwer skanowania dostarczony w formie gotowego obrazu (appliance) dla środowisk HyperV oraz Vmware

Zdalne administrowanie ochroną

1. Integracja z Active Directory - import kont komputerów i jednostek organizacyjnych.
2. Ochrona dla urządzeń z systemem Android.

3. Zarządzanie urządzeniami z systemem iOS.
4. Przenośna konsola administracyjna pobierająca interfejs zgodny z serwerem zarządzającym.
5. Opcja automatycznej instalacji oprogramowania klienckiego na wszystkich podłączonych komputerach Active Directory.
6. Zdalna instalacja i centralne zarządzanie klientami na stacjach roboczych i serwerach Windows.
7. Zdalna instalacja i centralne zarządzanie klientami Linux / OS X.
8. Do instalacji zdalnej i zarządzania zdalnego nie jest wymagany dodatkowy agent. Na końcówkach zainstalowany jest sam program antywirusowy.
9. Możliwość zarządzania ochroną urządzeń mobilnych z poziomu konsoli (przynajmniej aktualizacje, ochronę przeglądarek, skanowania zasobów, synchronizacji raportów).
10. Możliwość kontekstowego zastosowania ustawień danej stacji dla całej grupy.
11. Możliwość eksportu/importu ustawień dla stacji/grupy stacji.
12. Możliwość zarządzania dowolną ilością serwerów zarządzających z jednego okna konsoli.
13. Możliwość zarządzania różnymi wersjami licencyjnymi oprogramowania producenta z jednego okna konsoli.
14. Możliwość tworzenia hierarchicznej struktury serwerów zarządzających (serwer główny i serwery podrzędne).
15. Możliwość zainstalowania zapasowego serwera zarządzającego, przejmującego automatycznie funkcje serwera głównego w przypadku awarii lub odłączenia serwera głównego.
16. Możliwość zdalnego zarządzania serwerem spoza sieci lokalnej przy pomocy połączenia VPN.
17. Możliwość zarządzania ochroną sieci wielu usługobiorców z poziomu jednej instancji serwera zarządzającego.
18. Szyfrowanie komunikacji między serwerem zarządzającym a klientami.
19. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
20. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania).
21. Możliwość przeglądania list programów zainstalowanych na stacjach/serwerach (nazwa, wersja, producent, data instalacji).
22. Możliwość stworzenia białej i czarnej listy oprogramowania, i późniejsze filtrowanie w poszukiwaniu stacji je posiadających.
23. Odczyt informacji o zasobach sprzętowych stacji (procesor i jego taktowanie, ilość pamięci RAM i ilość miejsca na dysku/partycji systemowej).
24. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
25. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.
26. Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów.
27. Możliwość zmiany konfiguracji na stacjach i serwerach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne).
28. Możliwość generowania raportów w formacie XML.
29. Możliwość przeglądania statystyk ochrony antywirusowej w postaci tekstu lub wykresów.
30. Możliwość przesłania komunikatu, który wyświetli się na ekranie wybranej stacji roboczej lub grupie stacji roboczych.
31. Komunikat można wysłać do wszystkich lub tylko wskazanego użytkownika stacji roboczej.

32. Możliwość zminimalizowania obciążenia serwera poprzez ograniczenie ilości jednoczesnych procesów synchronizacji, aktualizacji i przesyłania plików do stacji roboczych.
33. Możliwość dynamicznego grupowania stacji na podstawie parametrów: nazwa komputera, adres IP, brama domyślna, nazwa domeny.

Raporty

1. Możliwość utworzenia raportów statusu ochrony sieci.
2. Możliwość generowania raportów w przynajmniej 3 językach.
3. Możliwość wysyłania raportów z określonym interwałem.
4. Możliwość wysłania jednego raportu na różne adresy mailowe lub grupy adresów.
5. Możliwość zdefiniowania przynajmniej 15 różnych typów informacji dotyczących statusu ochrony oraz różnych form ich przedstawienia (tabele, wykresy) w pojedynczym raporcie.

Osobista zapora połączeń sieciowych

1. W pełni zdalna instalacja, zdalne zarządzanie wszystkimi funkcjami zapory i zdalna deinstalacją.
2. Zapora działająca domyślnie trybie automatycznego rozpoznawania niegroźnych połączeń i tworzenia reguł bez udziału użytkownika.
3. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
4. Możliwość interakcji między użytkownikiem a administratorem w celu dostosowania zestawu reguł.
5. Możliwość zdefiniowania osobnych zestawów reguł dla dowolnych grup użytkowników.
6. Wbudowany system IDS.
7. Możliwość pracy w trybie offsite po odłączeniu od sieci przedsiębiorstwa.
8. Wykrywanie zmian w aplikacjach korzystających z sieci na podstawie sum kontrolnych i monitorowanie o tym zdarzeniu.
9. Możliwość automatycznego skanowania antywirusowego modułów o zmodyfikowanych sumach kontrolnych.
10. Automatyczne wysyłanie powiadomień o zablokowaniu aktywności sieciowej na wskazany adres mailowy.
11. Import/eksport reguł/zestawów reguł zapory na stacji roboczej.

Zdalne zarządzanie wydajnością i czasem pracowników (PolicyManager)

1. Wszystkie obostrzenia modułu można zastosować zarówno wobec użytkowników z ograniczonymi kontami Windows, jak i administratorów.
2. Kontrola aplikacji umożliwiająca blokowanie lub zezwalanie na stosowanie konkretnych programów, folderów i plików. Opcja zablokowania pliku w konkretnej wersji, o danej sumie kontrolnej oraz podpisanego cyfrowo przez wskazanego producenta.
3. Kontrola urządzeń pozwalająca na zarządzanie dostępem do napędów CD/DVD/BD, pendrive'ów, dysków oraz kamer USB, a także tradycyjnych stacji dyskietek. Możliwe jest zablokowanie urządzenia a także ustawienie dostępu tylko do odczytu.
4. Możliwość wykluczenia urządzeń na podstawie ich numeru ID i nadanie im pełnych uprawnień lub tylko do odczytu.
5. W przypadku wykluczeń urządzeń możliwe jest napisanie odpowiedniego komentarza dla danego wyjątku.
6. Kontrola treści internetowych umożliwiająca zablokowanie/odblokowanie użytkownikom stron internetowych z konkretnych kategorii. Rozbudowana lista aktualizowana jest przez Internet.
7. Biała i czarna lista stron internetowych stosowana bez względu na przypisaną im kategorię treści.

8. Kontrola czasu spędzanego w Internecie. Możliwość precyzyjnego określenia w jakich godzinach jakiego dnia użytkownik może przeglądać treści internetowe. Dodatkowo można określić dzienny, tygodniowy oraz miesięczny limit czasu przeznaczonego do korzystania ze stron internetowych.
9. Po zablokowaniu aplikacji, urządzenia lub strony internetowej użytkownik może zażądać udostępnienia zablokowanego zasobu wprost z okna z komunikatem o blokadzie.
10. Administrator ma możliwość odblokowania zasobu z poziomu raportu konsoli zarządzającej utworzonego automatycznie po zaznaczeniu przez użytkownika opcji zażądania dostępu do zablokowanego zasobu.
11. Automatyczne wysyłanie powiadomień o zablokowaniu danego zasobu na wskazany adres mailowy.